Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

An unending variety of topics

Tuesday, September 04, 2007

Secure property titles

From Secure Property Titles with Owner Authority:

> In all cases of property rights there is a defined space, whether a namespace or physical space, and the task is to agree on simple attributes of or rights to control subdivisions of that space. In some cases a name or other symbol corresponds to a person or object owned or controlled by that person. For example, Internet users must agree on which domain name corresponds to which web site operator. In other cases we are simply concerned with control over a subdivision of the space. With real estate we must agree on who owns various rights (to occupy the surface, to mine the minerals under, etc.) to a piece of land. With radio spectrum we must agree on who owns what range of frequencies and in what physical space (or transmitting power as an easily observed approximation of physical space used).
>
> ...all such [multiparty problems of] control over the semantics of symbols, to be made and respected across trust boundaries, are problems of agreeing on and maintaining property rights...
>
> ...New advances in replicated database technology will give us the ability to securely maintain and transfer ownership for a wide variety of kinds of property, including not only land but chattels, securities, names, and addresses. This technology will give us public records which can "survive a nuclear war", along the lines of the original design goal of the Internet. While thugs can still take physical property by force, the continued existence of correct ownership records will remain a thorn in the side of usurping claimants...
>
> The ideal title database would have the following properties:
>
> (1) Current owner Alice should be able transfer her title to only a single relying counterparty (similar to the "double spending" problem in digital cash)
>
> (2) Servers should not be able to forge transfers
>
> (3) Servers should not be able to block transfers to or from politically incorrect parties.
>
> ...Using these results [of Byzantine quorum systems] it looks like we can approach our ideal title database as follows:

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

(1) Alice signs the title and Bob's public key, and sends this message to 2f+1 servers, committing her to transfer title to Bob. Bob checks at least 2f+1 servers before relying on Alice's transfer.

(2) No collusion of servers can forge Alice's signature (we achieve at least this property ideally!)

(3) A conspiracy of >=(1/4)n servers can block a transfer. Alice's recourse is to use some other channels to broadcast her intention, demonstrating that the registry did not follow her wishes, and hoping the alternative channels are more reliable. Bob only has similar recourse if he signed a document with Alice demonstrating their intentions to transfer title from Alice to Bob. The most basic recourse is a correct subset of servers which exits the property club and establishes a new one, then advertises its correctness (and proves the incorrectness of its rival group) as described above.

More here.

Posted by Nick Szabo at 5:26 PM

1 comment:

blastomere said...

I wonder if the proxy signatures you described a few blog posts ago would be helpful for giving agents authority to buy/sell property titled in this way.

4:21 PM

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ▼ 2007 (47)
  - ► December (1)
  - ► October (2)
  - ▼ September (8)
    - Secure time broadcast
    - Real options analysis for space projects
    - Tamper evident numbers
    - Mining the vasty deep (iii)
    - Partial and total orders
    - Institutional changes prerequisite to the industri...
    - Secure property titles
    - Bilinear group cryptography
  - ► August (10)
  - ► July (4)
  - ► June (4)
  - ► May (8)
  - ► April (1)
  - ► March (2)
  - ► February (4)
  - ► January (3)
- ► 2006 (130)
- ► 2005 (44)

Simple theme. Powered by Blogger.